Final Concluding Activity: Integrated Security Evaluation of Capstone System

Title: Security Architecture Audit & Defense Presentation: Applying IAS2 Concepts to Your Capstone System”

Learning Outcomes Verified

This concluding activity confirms that students can:

- Integrate ALL security concepts from the subject
- Apply cybersecurity principles in real-world systems
- Communicate security design professionally
- Produce a system aligned with industry security standards

Purpose of the Activity:

This concluding activity will verify how you understand and apply the full scope of **Information Assurance and Security 2** by **connecting the concepts to your own capstone system**.

You will present how your system addresses the following areas:

- Cryptography
- Network Security Architecture
- Identity and Access Management
- Security Monitoring and Operations
- Cloud & Virtualization Security
- Legal, Ethical, Regulatory Compliance
- Emerging Threats & Defensive Strategies

This ensures that your capstone is **not only functional but secure**, meeting real-world requirements.

Activity Description

Each group must conduct a **Security Audit & Defense Presentation** of their capstone system. You will present:

1. System Overview (3–5 minutes)

- Name of system
- Purpose and target users
- Architecture (basic block diagram)
- Technologies used

2. Security Implementation Mapping (Core Part)

The group must explain how their system implements (or plans to implement) the required security measures.

Below is the checklist you must follow:

A. Cryptographic Controls

Students must show (choose what applies):

- What data needs encryption (passwords, personal data, transactions, logs)?
- Which algorithms or protocols were used (AES, RSA, SHA-256, HMAC, TLS)?
- How keys are generated, stored, or exchanged

- How integrity is maintained (hashing, digital signatures)
- How they avoid common cryptographic attacks

B. Network Security Architecture

Explain:

- Network topology of the system (local app, cloud, hosted server, hybrid)
- Security zones (DMZ, internal network, public interface)
- Firewall rules, filters, or segmentation strategies
- How they apply **defense-in-depth**, least privilege, fail-safe defaults
- Use of HTTPS, SSL/TLS, VPN, or secure communication

C. Identity and Access Management (IAM)

They must present:

- Authentication implemented (password, OTP, biometrics, tokens, SSO)
- Authorization model used (RBAC, ABAC, DAC)
- Password policy, MFA requirement, and account lockout
- IAM lifecycle (account creation, role change, termination)
- Privileged access safeguards

D. Security Monitoring and Operations

Students must demonstrate:

- What logs the system generates
- How are logs stored (centralized? encrypted?)
- How they detect anomalies or attacks
- Use of SIEM-like logic (even simplified version)
- Incident response plan for their system
- Vulnerability and patch management approach

E. Cloud / Virtualization Security (if applicable to their system)

Explain:

- Cloud model (IaaS/PaaS/SaaS) and deployment model
- Shared responsibility model
- Cloud security settings (ACLs, security groups, encryption)
- VM/container security
- Misconfiguration prevention
- Backup and disaster recovery plan

F. Legal, Ethical & Regulatory Compliance

They must map their system to:

  - Data Privacy Act of 2012 (PH)
  - GDPR principles (if applicable)
  - Ethical data handling
  - Consent, data retention, lawful processing
  - Audit trails and accountability
- Compliance with intellectual property laws

G. Emerging Threats and Modern Security Trends

Students should identify:

- Potential threats their system faces (ransomware, phishing, MITM, DoS)
- Modern defense strategies that they applied
- How Zero Trust, micro-segmentation, AI-based detection, and API security apply
- How their system stays secure for the next 3–5 years

3. Security Gaps & Improvement Plan

Students must present:

- 3–5 security vulnerabilities found in their system
- Proposed mitigation strategies
- Possible future implementation (ZTA, MFA, SIEM integration, encryption improvements, etc.)

4. Final Presentation Format

Duration: 15–18 minutes

- 5 minutes – System Overview
- 10 minutes – Security Mapping (A–G)
- 3 minutes – Security Gaps & Improvement Plan

Materials Required

- PowerPoint presentation
- Optional demo of the system
- System architecture diagram

6. Output Submission

Students must submit:

- **Security Audit Report (PDF)**
- **Presentation Slides (PPT)**
- **Updated Data Flow Diagram with security layers**

Sample Final Output: Security Audit & Defense Presentation

System Chosen: *LAZADA E-Commerce Platform* (Sample Only)

---

1. System Overview

System Name: Lazada E-Commerce Platform

Purpose:

To provide an online marketplace where customers can browse products, place orders, and complete secure digital transactions.

Target Users:

- Buyers
- Sellers
- Delivery Partners
- Administrators

System Architecture (Simplified):

- Frontend (Web & Mobile App)
- Backend API
- Database Cluster (User Data, Orders, Inventory)
- Payment Gateway (3rd Party + In-App Wallet)
- Content Delivery Network (CDN)
- Cloud Infrastructure (AWS)

2. Security Implementation Mapping (A–G)

A. Cryptographic Controls

Data Encryption

- Sensitive Data at Rest:
  - User passwords hashed using bcrypt (SHA-2 family)
  - Payment tokens encrypted using AES-256
- Data in Transit:
  - All communication uses HTTPS with TLS 1.3
  - API calls use HMAC signatures

Key Management

- Keys stored in **AWS KMS (Key Management Service)**
- Regular key rotation every 90 days

Integrity & Non-Repudiation

- Digital signatures on API transactions
- Hashing is used for file uploads and product images

Defense Against Cryptographic Attacks

- Salted password hashing prevents rainbow table attacks
- TLS prevents MITM, downgrade, and replay attacks

B. Network Security Architecture

Network Segmentation

- **Public Zone:** Customer-facing portal
- **DMZ:** API gateway, CDN endpoints
- **Private Zone:** Databases, authentication services
- **Admin Zone:** Internal dashboards

Firewalls & Access Control

- WAF filters SQL injection, XSS, request floods
- Rate limiting to prevent brute-force & DoS
- Network ACLs block unauthorized IP ranges

Secure Communication

- HTTPS, TLS 1.3
- VPN for admin access
- Hardened SSH for server maintenance

Defense-in-Depth

- Multi-layered firewalls + IDS + SIEM
- Continuous patching and vulnerability scans

C. Identity and Access Management (IAM)

Authentication

- Buyers & Sellers:
  - Username + password
  - Optional **MFA via SMS/Authenticator App**
- Admin Accounts:
  - **Mandatory MFA**
  - Device fingerprinting

Authorization

- Uses **RBAC (Role-Based Access Control)**
- Roles: Buyer, Seller, Delivery Rider, Admin, Super Admin
- Sellers cannot access buyer data; Admins cannot see card details

IAM Lifecycle

- Seller onboarding includes ID verification
- Automated account lockout after failed attempts
- Account deactivation after long inactivity

Privileged Access Management

- Admin activities logged
- Session recording for sensitive actions

D. Security Monitoring & Operations

Logging

- Login events
- Payment activities
- Failed login attempts
- Seller product changes
- Admin actions

SIEM Integration

- Logs go to **AWS CloudWatch + Elastic SIEM**
- Correlation rules detect:
    - Suspicious IPs
    - Sudden spike in orders
    - Fraudulent transactions

Incident Response Workflow

1. Detect
2. Analyze
3. Contain
4. Recover
5. Document

Vulnerability & Patch Management

- Weekly scans for misconfigurations
- Monthly patching window
- Bug bounty program

E. Cloud & Virtualization Security

Cloud Deployment

- **AWS Hybrid Cloud** (EC2 + S3 + RDS)
- **Shared Responsibility Model Followed**

Cloud Security Controls

- IAM roles for services
- Security groups per microservice
- S3 buckets encrypted (AES-256)
- CloudTrail for auditing

Virtualization Security

- Uses AWS EC2 instances with hardened AMIs
- Containerized microservices (Docker + Kubernetes)
- Prevents VM escape by limiting hypervisor access

Backup & Recovery

- Daily encrypted backups to S3

- DR site on another region
- RTO: 4 hours | RPO: 15 minutes

F. Legal, Ethical & Regulatory Compliance

Applicable Laws

- Data Privacy Act of 2012 (PH)
- Cybercrime Prevention Act of 2012
- GDPR (for international customers)

Data Subject Rights

- Users can request account deletion
- Consent collected for tracking & cookies

Audit & Compliance

- Yearly 3rd-party security assessment
- PCI DSS compliance for card payments
- Intellectual property compliance for seller products

Ethical Standards

- Transparent privacy policy
- Responsible disclosure program
- Anti-fraud and anti-scam mechanisms

G. Emerging Threats & Modern Defenses

Threats Identified

- AI-powered phishing targeting buyers
- Fake seller listings
- Credential stuffing
- Supply chain attacks on plugins/APIs
- DDoS attacks during sale events

Modern Defense Strategies

- AI-based anomaly detection
- Behavioral analytics
- Zero Trust for internal admin systems
- API Gateways with OAuth 2.0
- Bot detection using ML models

---

3. Security Gaps & Improvement Plan

Identified Weakness	Possible Impact	Mitigation
Some sellers use weak passwords	Account takeover	Enforce mandatory MFA

Identified Weakness	Possible Impact	Mitigation
Large number of third-party plugins	Supply chain attacks	Pen-test all plugins; reduce dependencies
Heavy traffic during double-digit sales	Risk of DDoS	Add auto-scaling and advanced WAF rules
Social engineering scams	Poor customer protection	More user education and fraud detection AI
Potential API abuse	Data leakage	Add stricter API throttling and OAuth scopes

Below is a **complete sample output for a Web-Based Booking System**, following your required concluding activity format.
This is ready to be given as a model/sample output for students.

Sample Final Output: Security Audit & Defense Presentation

System Chosen: *Web-Based Booking System* (Sample Capstone System)

1. System Overview

System Name:

EZBook – Web-Based Booking and Reservation Platform

Purpose:

To allow users to book appointments, reserve rooms/seats/services, view schedules, and manage reservations online.

Target Users:

- Customers
- Service Providers / Staff
- Administrators

System Architecture (Simplified):

- Web Frontend (HTML/CSS/JS)
- Backend Application (PHP / Node.js)
- MySQL / PostgreSQL Database
- Authentication & Session Server
- Admin Dashboard
- Cloud Hosting (AWS EC2 / Google Cloud VM)

---

2. Security Implementation Mapping (A–G)

A. Cryptographic Controls

Data Encryption

- **Data in Transit:**
    - HTTPS with **TLS 1.3**

- **Data at Rest:**
    - User passwords hashed using **bcrypt (SHA-256 family)**
    - Sensitive booking details (IDs, phone numbers) encrypted using **AES-256**

Key Management

- Keys stored in a secure configuration vault
- Key rotation every 90 days

Integrity & Digital Trust

- Hashing for uploaded attachments (PDF, receipts)
- HMAC signing for API communication (booking confirmations)

Protection from Crypto Attacks

- Salted password hashing (prevents rainbow tables)
- TLS prevents MITM and replay attacks
- Strong 2048-bit RSA for certificate exchange

B. Network Security Architecture

Network Segmentation

- **Public Zone:** Website, booking interface
- **Application Zone (DMZ):** API server
- **Private/Internal Zone:** Database, admin portal

Firewalls & Access Control

- WAF blocks SQL Injection, XSS, CSRF
- Rate-limiting for login and booking requests
- Only backend servers may access DB (via private subnet)

Secure Communication

- HTTPS enforced (no HTTP allowed)
- Hardened SSH (key-based authentication)

Defense-in-Depth Implementation

- Layered firewalls + IDS (Snort/Security Onion)
- Automated patching of OS and server software

C. Identity and Access Management (IAM)

Authentication

- Standard login (email + password)
- Optional **MFA (email OTP / Google Authenticator)**
- Session tokens secured with HttpOnly & Secure flags

Authorization

- **RBAC roles:**
    - Customer

  - Staff
  - Admin
- Staff cannot access admin reports
- Customers only view/manage their own bookings

Account Security

- Password strength requirement
- Email verification for new accounts
- Automatic account lockout after too many failed logins

Privileged Access Management

- Admin actions logged (audit trail)
- Access review every semester

D. Security Monitoring and Operations

Logging

System logs:

- Login attempts (success & failed)
- Booking modifications
- Cancelled reservations
- Admin configuration changes

Event Correlation (SIEM-like process)

- Logs sent to a central logging server
- Alerts triggered for:
  - High failed login count
  - Suspicious IP attempting bookings
  - Staff accessing data outside their working hours

Incident Response Plan

1. Detect unusual activity
2. Analyze logs
3. Contain (lock user or disable booking functions)
4. Recover (restore system or data)
5. Document incident

Patch Management

- Weekly OS updates
- Monthly vulnerability scanning
- Use of OWASP security checklist

E. Cloud & Virtualization Security

Cloud Deployment

- Hosted on AWS EC2 with RDS for database
- S3 used for storing attachments

Security Controls

- Security groups allow port 443 only
- IAM roles restrict access per service
- S3 buckets encrypted using SSE-S3
- CloudTrail logs for auditing
- Auto-backups enabled for database

Virtualization

- Hardened VM image
- Limited user accounts (root disabled for remote login)

Backup & Disaster Recovery

- Daily database backup
- Weekly full system image backup
- Failover instance in another region
- RTO: 4 hours | RPO: 30 minutes

F. Legal, Ethical & Regulatory Compliance

Applicable Laws

- Data Privacy Act of 2012 (PH)
- Cybercrime Prevention Act of 2012
- Privacy-by-design principle applied

Data Protection Practices

- Only necessary user data collected
- Users can modify or delete accounts
- Retention of logs limited to 6 months

Ethics

- Honest data usage disclosure
- Transparent privacy notice
- No hidden data-sharing practices

Audit & Compliance

- Quarterly internal security audit
- Compliance with OWASP Top 10
- Consent required before storing user details

G. Emerging Threats & Modern Security Defenses

Potential Threats

- Phishing attacks on customer logins

- Booking manipulation / fake bookings
- Bot attacks (automated mass reservations)
- Insider threats (disgruntled staff)
- DoS attacks on peak booking periods

Modern Defenses

- CAPTCHA for new bookings
- Bot detection (rate limit + user behavior analysis)
- Zero Trust approach for admin area
- AI-based anomaly detection for fraud bookings
- Regular pentesting using OWASP ZAP or Burp Suite

---

3. Security Gaps & Improvement Plan

Identified Weakness	**Impact**	**Mitigation**
No full MFA for all users	Account compromise	Make MFA mandatory
Staff reuse passwords	Insider risk	Enforce password rotation policies
API endpoints vulnerable to brute force	Unauthorized access	Add API throttling and IP blocking
Logs are not yet centralized	Slow detection of breaches	Use ELK Stack or a SIEM tool
Only daily backups	Possible data loss	Increase to 12-hour interval backup

---

Refer to this list on how to Present your work output

FINAL CONCLUDING ACTIVITY

Integrated Security Evaluation of Capstone System

1. System Overview

Each group must introduce its capstone system by presenting:

✓ Name of the System

Example: *Web-Based Booking System*, *Inventory Management System*, *LMS*, *Event Management App*, etc.

✓ Purpose of the System

Brief description of what the system does.

✓ Target Users

Who uses the system (customers, staff, admins, etc.)

✓ System Architecture (Basic Block Diagram)

At minimum, it must show:

- Frontend
- Backend

- Database
- External services / APIs
- Hosting (local server or cloud)

✓ Technologies Used

Examples: PHP, Python, Node.js, MySQL, Firebase, AWS, Docker, etc.

---

2. SECURITY IMPLEMENTATION MAPPING (CORE PART)

📌 **The heart of the presentation.**

Students must explain **how their system applies the security concepts** from ALL modules in IAS2.

They must explicitly discuss the following areas:

A. Cryptography

Students must explain:

- What data is encrypted (passwords, personal info, payments, logs, etc.)
- Algorithms used (AES, RSA, SHA-256, bcrypt)
- How hashing and digital signatures are applied
- How data integrity is ensured
- How keys are generated, stored, and rotated
- Protection against common crypto attacks

B. Network Security Architecture

Students must present:

- System's network layout / zones (public, DMZ, internal, admin)
- Firewall rules, packet filtering
- Use of HTTPS, SSL/TLS, VPN
- Server hardening and segmentation (VLANs, subnetting)
- Defense-in-depth implementation
- Prevention of network attacks (MITM, DoS, ARP poisoning)

C. Identity and Access Management (IAM)

Students will explain:

- Authentication methods (password, OTP, MFA)
- Authorization model (RBAC, ABAC, DAC)
- Access control policies (least privilege, need-to-know)
- Password policy and account lockout
- Session management and timeout
- Privileged access handling (admins, super admins)
- Identity lifecycle management

D. Security Monitoring & Operations

Students must show:

- What logs the system records (logins, actions, errors, failed attempts)
- Where logs are stored and how long they are retained
- How incidents are detected and reported (alerts, thresholds, SIEM-like logic)
- Incident response process (detect → analyze → contain → recover → document)
- Vulnerability scanning and patch management plan

E. Cloud & Virtualization Security

(Required if system uses cloud or virtual machines)

Students must explain:

- Cloud service model (IaaS, PaaS, SaaS)
- Deployment model (public, private, hybrid)
- Shared responsibility model
- Cloud security controls (KMS, IAM roles, ACLs, encryption)
- VM/container security (Docker, VMs, snapshots)
- Backup and disaster recovery strategy

F. Legal, Ethical & Regulatory Compliance

Students identify:

- Applicable laws (Data Privacy Act of 2012, Cybercrime Law, GDPR)
- Data handling and consent mechanisms
- Data retention policies
- User rights (access, correction, deletion)
- Compliance with ethical standards
- Documentation and audit trail requirements

G. Emerging Threats & Defensive Strategies

Students will evaluate:

- Possible threats to their system (phishing, ransomware, SQLi, DDoS, credential stuffing, insider threats)
- Modern defenses applied (Zero Trust, MFA, AI-based detection, CAPTCHA, SIEM, hardened APIs)
- How the system remains secure for the next 3–5 years
- Risk assessment and preventive measures

End Goal

Students must prove that their capstone system is:

- Secure

- Compliant
- Well-designed
- Resistant to common attacks
- Scalable and future-proof

✅ 1. GRADING RUBRIC (Comprehensive & Final)

Final Concluding Activity: Security Architecture Audit & Defense Presentation

A. Group Performance – 70%

Criteria	Description	Points
Content Mastery	Accuracy, depth, and completeness of security concepts mapped to the capstone system	**20 pts**
Organization & Clarity	Logical flow, coherence, easy to follow presentation	**10 pts**
Creativity & Engagement	Quality of visuals, diagrams, activities, demo, audience engagement	**10 pts**
Security Implementation Mapping (A–G)	How well the team applied all IAS2 topics to their system	**15 pts**
Visual Aids	Clean PPT design, readable text, diagrams, proper formatting	**10 pts**
Time Management	Presented within 15–18 minutes, smooth transition	**5 pts**

Subtotal: 70 points

B. Individual Performance – 30%

Criteria	Description	Points
Participation	Contribution in presentation and preparation	**10 pts**
Communication Skills	Clarity, confidence, proper pacing, eye contact	**10 pts**
Teamwork & Cooperation	Coordination, respect, initiative	**10 pts**

Subtotal: 30 points

TOTAL: 100 POINTS

✅ 2. FULL SAMPLE OUTPUT (Web-Based Booking System)

This is a complete student-quality sample they can follow.

You can provide this as an example but instruct them **not to copy**.

Sample Final Output – Web-Based Booking System

1. System Overview

- **System Name:** Booking Online Booking Platform

- **Purpose:** Allows customers to create bookings, check availability, cancel schedules, and receive confirmations.
- **Target Users:** Customers, Staff, Admin
- **Architecture:**
  - Frontend: HTML/CSS/JS
  - Backend: PHP or Node.js
  - DB: MySQL
  - Hosting: AWS EC2
- **Technologies:** Bootstrap, JWT, bcrypt password hashing, TLS 1.3 enabled hosting.

---

2. Security Implementation Mapping (A–G)

A. Cryptography

- TLS 1.3 for secure data transfer
- AES-256 for encrypting sensitive booking notes
- bcrypt hashing for passwords
- HMAC verification for API calls

B. Network Security Architecture

- 3-layer network: Public → DMZ → Private
- WAF blocks SQLi, XSS
- Firewall rules restrict DB access
- Rate limiting enabled

C. Identity and Access Management

- RBAC: Customer, Staff, Admin
- MFA optional
- Session timeout & secure cookies
- Account lockout after 5 failed attempts

D. Security Monitoring & Operations

- Logs: login, booking changes, admin actions
- Centralized log storage
- Alerts for suspicious IPs or failed logins
- Weekly vulnerability scans

E. Cloud & Virtualization Security

- AWS EC2 + RDS
- Security groups enforce least privilege
- Encrypted backups (daily)
- IAM roles for cloud services

F. Legal & Ethical Compliance

- Data Privacy Act of 2012
- Consent for data collection

- Data retention policy (180 days logs)
- Secure deletion process for accounts

G. Emerging Threats & Defensive Strategies

- CAPTCHA to prevent bot bookings
- Zero Trust for admin access
- AI-based anomaly detection planned
- Anti-DoS rate limits enabled

---

3. Gaps & Mitigation

Gap	Risk	Fix
No forced MFA	Account takeover	Require MFA for staff & admin
Manual log review	Slow response	Implement automated alerts
Single region backup	Downtime risk	Multi-region DR strategy

Sample Completed.

Students should produce something similar.

---

3. STUDENT TEMPLATE

STUDENT TEMPLATE — FINAL OUTPUT

Security Architecture Audit & Defense Presentation

Group Name:
System Title:
Course: IAS2
Instructor:

---

1. System Overview

- System Name:
- Purpose:
- Target Users:
- System Description:
- System Architecture Diagram (Insert Image)
- Technologies Used:

---

2. Security Implementation Mapping (A–G)

A. Cryptography

- Encryption at rest:
- Encryption in transit:
- Hashing:
- Key management:

B. Network Security Architecture

- Network topology:
- Firewalls / filters:
- Secure communication:
- Defense-in-depth:

C. Identity & Access Management

- Authentication:
- Authorization:
- Password policies:
- Privileged access:

D. Security Monitoring & Operations

- Logs collected:
- Monitoring tools:
- Incident response flow:
- Patch management:

E. Cloud & Virtualization Security

- Cloud model:
- Virtualization security:
- Backup & DR:

F. Legal, Ethical & Regulatory Compliance

- Laws applied:
- Data handling:
- Retention & disposal:

G. Emerging Threats & Defensive Strategies

- Possible threats:
- Modern defenses:
- Future-proofing plan:

---

3. Security Gaps & Mitigation Plan

Weakness	Impact	Proposed Solution

---

4. Conclusion

Short summary of the system’s overall security posture.

---

5. References

---

4. POWERPOINT OUTLINE (For Their Defense Presentation)

Slide 1 – Title Slide

- System Name
- Group Members
- Course, Date

Slide 2 – Introduction

- Purpose of the system
- Target users

Slide 3 – System Architecture

- Architecture diagram
- Technologies used

Slide 4 – Cryptography

- Encryption (AES, TLS)
- Hashing (bcrypt)
- Key management

Slide 5 – Network Security Architecture

- Network diagram
- Firewalls, IDS/IPS
- Defense layers

Slide 6 – Identity & Access Management

- RBAC roles
- MFA, password policies
- Session security

Slide 7 – Security Monitoring

- Logs
- Alerts
- Incident response

Slide 8 – Cloud & Virtualization Security

- Hosting
- Virtual machine/container security
- Backup & DR

Slide 9 – Legal & Ethical Compliance

- Data Privacy Act
- Consent & retention
- Compliance requirements

Slide 10 – Emerging Threats

- Ransomware
- Bot attacks
- API exploitation
- Mitigation strategies

Slide 11 – Security Gaps

- Table of weaknesses

Slide 12 – Recommendations

- Improvements and enhancements

Slide 13 – Conclusion

- Final evaluation of system security

!